Claims

WHAT IS CLAIMED IS:

1. A method for authenticating a principal, comprising:

receiving an access request from a first principal for access to a second principal;

evaluating a contract to acquire a credential for the first principal; and

transmitting the credential to the first principal for use in interacting with the second principal, wherein the credential includes authentication information, aggregated attributes and aggregated policies for use by the first principal in interacting with the second principal.

2. The method of claim 1 further comprising determining if the first principal is authenticated based on the contract and if the first principal is not authenticated establishing an authentication session with the first principal to properly authenticate the first principal based on the contract.

3. The method of claim 1 further comprising:

receiving an additional access request from the first principal for access to a third principal;

evaluating a new contract to acquire a second credential for the first principal; and

transmitting the second credential to the first principal for use in interacting with the third principal.

4. The method of claim 1 further comprising removing the contract or revoking the credential when an expiring event is detected during a session with the first principal.

5. The method of claim 1 further comprising:

receiving a new request from a third principal, wherein the new request desires attribute information associated with the first principal;

acquiring a new contract for the third principal;

evaluating the new contract to acquire a new credential for the third principal; and

transmitting the new credential to the third principal for use in authenticating and interacting with the first principal to acquire the attribute information.

6. The method of claim 1 further comprising:

receiving a modification to the contract from the first principal;

determining if the modification is permissible according to the contract;

updating the contract if the modification is permissible;

deriving a modified credential from the contract; and

transmitting the modified credential to the first principal for use in interacting with the second principal.

7. The method of claim 1 further comprising:

receiving a new request from the first principal for establishing a trust relationship with the second principal, wherein the trust relationship is established via communications having public-private key pairs between the first principal and the second principal;

determining if the trust relationship is permissible;

receiving a dynamically generated public key from the first principal associated with a dynamically generated private key, the dynamically generated private key maintained by the first principal; and

making the dynamically generated public key accessible to the second principal.

8. The method of claim 7 further comprising:

receiving from a third principal a static rooted public key associated with the

second principal; and

transmitting the static rooted public key to the first principal for use in interacting with the second principal in the trust relationship.

9. A method for authenticating a principal, comprising:

receiving first requests from a first principal to interact with one or more different principals;

acquiring first contracts for the first principal, wherein each first contract is associated with a different one of the one or more different principals;

acquiring a second contract for each of the one or more different principals;

selectively assembling and transmitting first credentials for the first requests for use by the first principal in interacting with the one or more different principals; and

selectively assembling and transmitting second credentials for other requests associated with and used by the one or more different principals when interacting with the first principal or when interacting with different ones of the one or more different principals.

10. The method of claim 9 further comprising:

receiving modifications to one or more of the first contracts from the first principal or from one or more of the one or more different principals;

selectively assembling and transmitting modified first credentials to the first principal based on the modifications.

11. The method of claim 9 further comprising:

receiving modifications to one or more of the second contracts from the first principal or from the one or more of the one or more different principals;

selectively assembling and transmitting modified second credentials to the one or more different principals affected by the modifications.

12. The method of claim 9 further comprising:

detecting an event that renders one or more of the first or second contracts stale; and

revoking one or more of the first or second credentials which are affected by the event.

13. The method of claim 9 wherein the selectively assembling of the first and second credentials further includes:

acquiring appropriate authentication certificates for each of the first and second credentials; and

acquiring aggregated attribute information and aggregated policies for each of the authentication certificates.

14. The method of claim 13 further comprising, expressing the authentication certificates within the first and second credentials as assertions.

15. The method of claim 13 wherein the acquiring the authentication certificates, the aggregated attribute information, and the aggregated policies further include accessing one or more identity stores having authentication information, attributes, and access policies associated with the first principal and the one or more different principals.

16. A principal authentication system, comprising:

a first principal service;

a second principal service; and

an identity service, wherein the identity service acquires and manages a first contract on behalf of the first principal service and a second contract on behalf of the second principal service, and wherein the identity service provides a first credential to the first principal service and a second credential to the second principal service, the credentials used by the first principal service and the second principal service to interact with one another.

17. The principal authentication system of claim 16 wherein the first or the second credential is dynamically modified by the identity service and communicated to the affected principal service.

18. The principal authentication system of claim 17 wherein the dynamic modification to the first or the second credential is driven by modifications received from the first principal service or the second principal service.

19. The principal authentication system of claim 17 wherein the dynamic modification to the first or the second credential is driven by modifications received from a third principal service authorized to provide the dynamic modification.

20. The principal authentication system of claim 16 wherein the identity service includes alias identity information in at least one of the first and the second credentials.

21. The principal authentication system of claim 16 wherein the first and second credentials include a first certificate for the first principal and a second certificate for the second principal, the certificates include identity information and techniques for authenticating the first and second principals.

22. The principal authentication system of claim 21 wherein the first and second credentials further include aggregated attribute information and aggregated policies for the first and second principals, the aggregated attribute information identifying types of data associated with the first and second principals and the aggregated policies defining operations which are permissibly performed or not permitted during the first and the second principal interactions.

23. A principal authentication system, comprising:

one or more identity stores; and

an identity service;

wherein the identity service dynamically establishes and manages authentication and interactions for a plurality of principals with respect to sessions occurring between the principals, the identity service acquires contracts for each of the principals and dynamically assembles one or more credentials for each of the principals for use in the sessions with one another, the one or more credentials assembled from the one or more identity stores based on the contracts.

24. The principal authentication system of claim 23 wherein the identity service substitutes alias identity information for identity information included within a number of the credentials.

25. The principal authentication system of claim 24 wherein the identity service updates one or more of the identity stores with the alias identity information.

26. The principal authentication system of claim 23 wherein the credentials include authentication certificates used for authentication the principals to one another during the sessions.

27. The principal authentication system of claim 26 wherein the credentials further include selective aggregated attributes and aggregated policies acquired from the one or more identity stores according to the contracts, the selective aggregated attributes identify types of data associated with the principals, and the selective aggregated policies identify at least one of permissible operations and non-permissible operations that can be processed against the selective aggregated attributes during the sessions between the principals.

28. The principal authentication system of claim 23 further comprising a trust data store associated with the identity service and separate trust data stores associated with each of the principals, wherein the identity service manages the trust data store and authorizes the principals to dynamically update their respective

separate trust data stores with selective identities and key information associated with the principals during the sessions between the principals.

29. The principal authentication system of claim 23 wherein the identity service communicates modified credentials to the principals during interactions between the principals.

30. The principal authentication system of claim 23 wherein the identity service revokes a number of the credentials for the principals when expiring events are detected.